

GeekBrains

Урок 3 Видео 1

Криптография

Обзор криптографических хеш-функций

В этом видео

1. Криптографический хеш
2. Свойства криптографических хеш-функций
3. Современные криптографические хеш-функции

Зачем нужны хеш-функции?

Хранение хешей от паролей вместо паролей

Гарантия неизменности файла

Кэш, криптографические схемы, …

Хеш-функция

Функция, которая превращает произвольную строку (данные) в строку фиксированной длины.





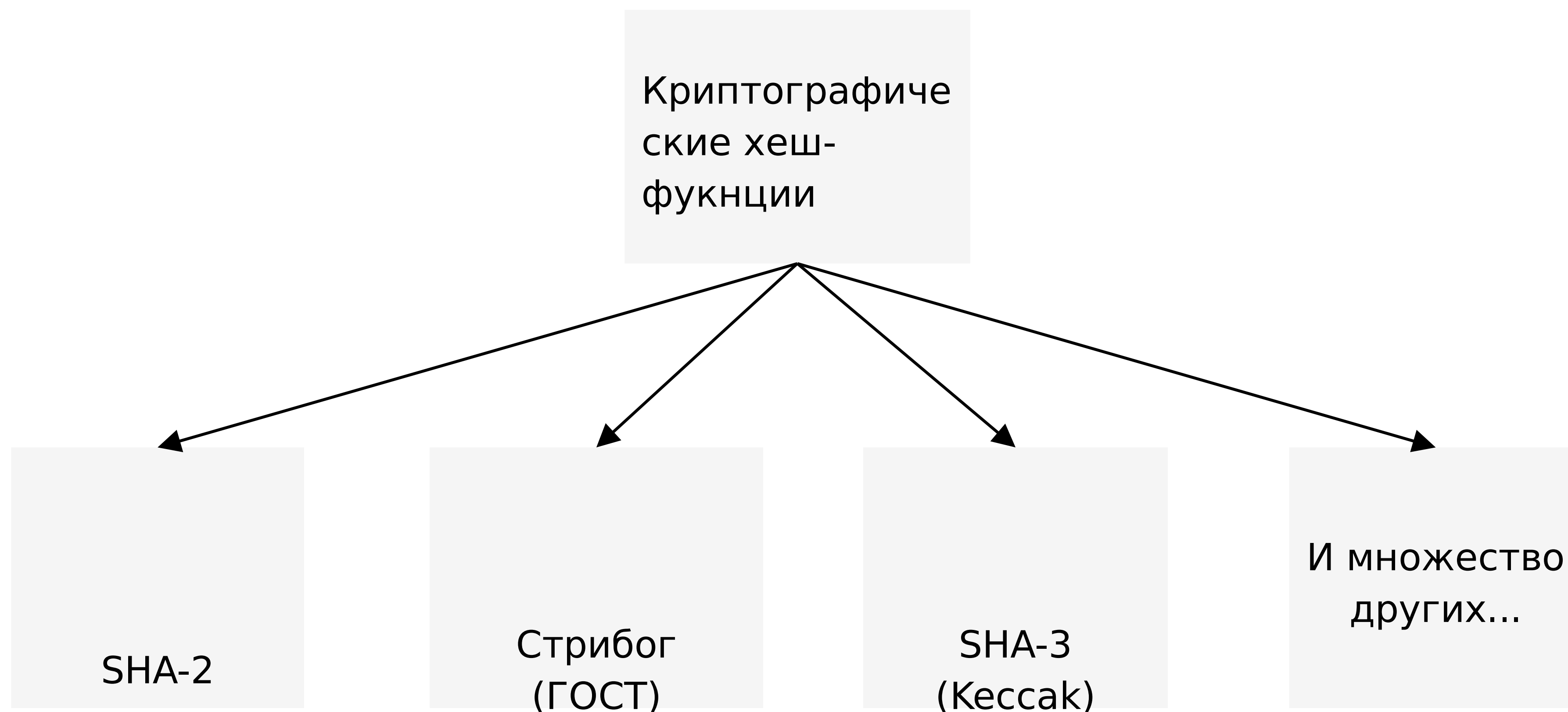
Свойства крипто хеш-функций

Зная хеш вычислительно сложно найти исходное сообщение

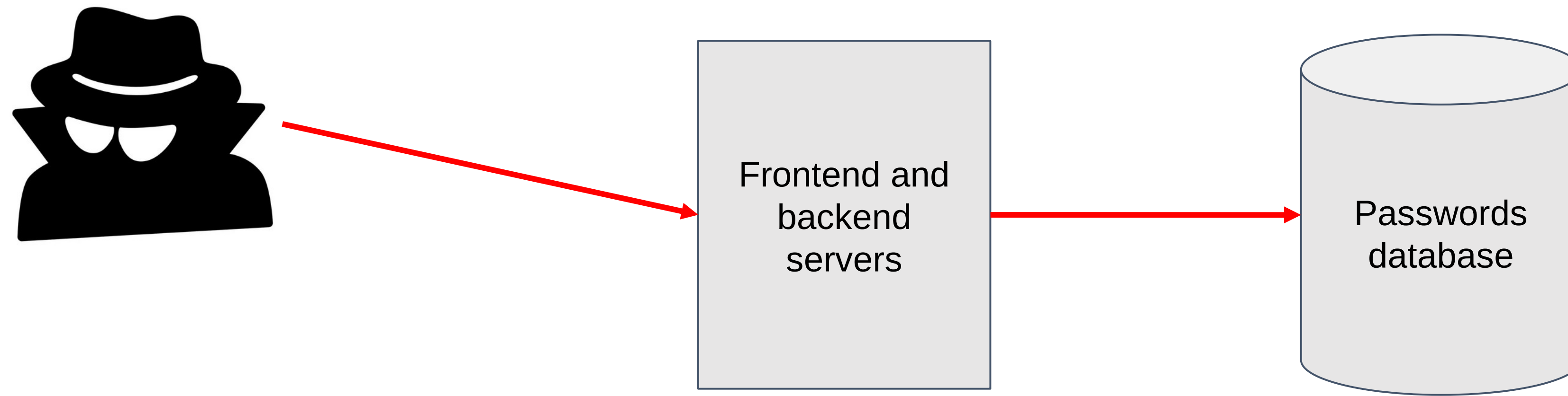
Вычислительно сложно найти коллизию

Вычислительно сложно, имея m1, найти m2, такое что h(m1) = h(m2)

Современные крипто хеш-функции



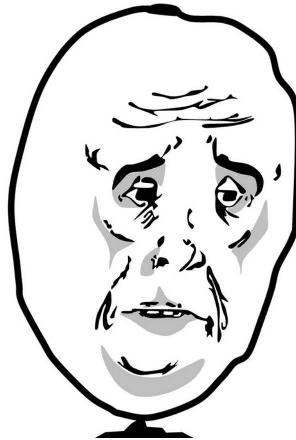
Хранение паролей в открытом тексте

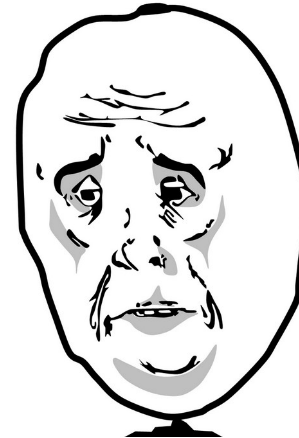


Хранение паролей в открытом тексте

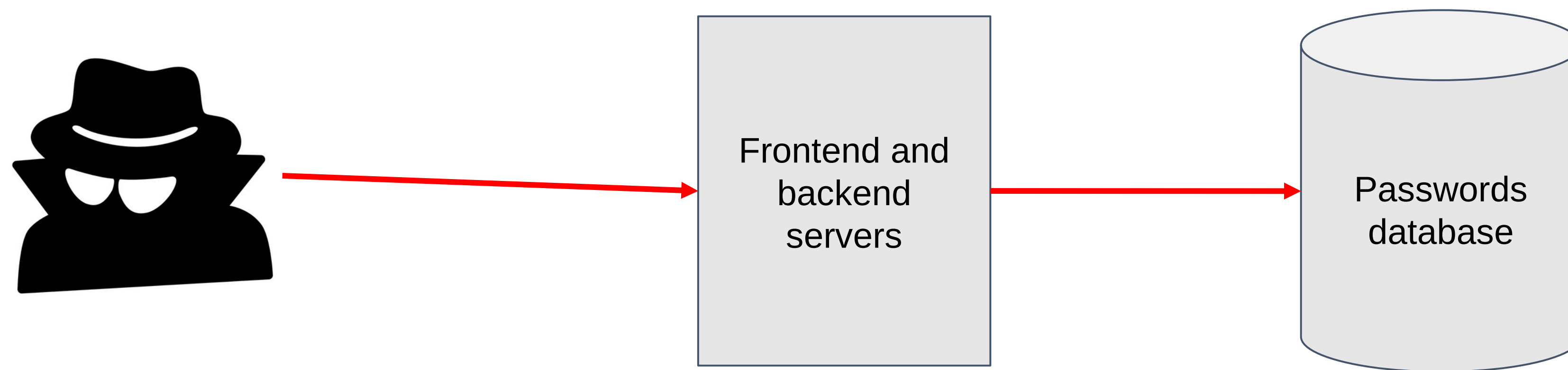


123456789
password
iloveyou
…

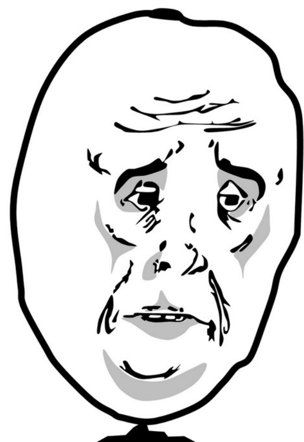




Хранение хешей от паролей



Хранение хешей от паролей



Frontend and backend servers

Passwords database

f447b20a7fcbf53a5d5be013ea0b15af
d577273ff885c3f84dadb8578bb41399
b2cfa4183267af678ea06c7407d4d6d8
…

Итоги

1. Узнали что такое криптографический хеш и зачем он нужен
2. Узнали свойства криптографических хеш-функций
3. Научились использовать криптографические хеш-функции в командной строке и в Python